(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－224053

(43)公開日　平成９年(1997)８月26日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　12/66		9466－5K	Ｈ０４Ｌ　11/20	Ｂ	
Ｇ０６Ｆ　13/00	３５１		Ｇ０６Ｆ　13/00	３５１Ｚ	

審査請求　未請求　請求項の数８　ＦＤ　（全 17 頁）

(21)出願番号　特願平8－147881

(22)出願日　平成８年(1996)５月20日

(31)優先権主張番号　４４４３５１

(32)優先日　1995年５月18日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　591064003
サン・マイクロシステムズ・インコーポレーテッド
SUN MICROSYSTEMS, INCORPORATED
アメリカ合衆国　94043　カリフォルニア州・マウンテンビュー・ガルシア　アヴェニュウ・2550

(72)発明者　ジェフリー・ジイ・ベール
アメリカ合衆国　94025　カリフォルニア州・メンロ　パーク・ケンブリッジ　アヴェニュ・628

(74)代理人　弁理士　山川　政樹

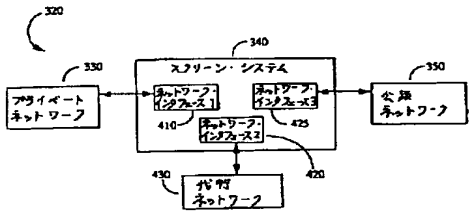
最終頁に続く

(54)【発明の名称】　コンピュータ・ネットワーク・インタフェースにおけるデータ・パケットのパケット・フィルタリング・システム

(57)【要約】

【課題】　プライベート・ネットワークなどの保護するネットワークと公衆ネットワークなどの他のネットワークとの間で伝送されるデータ・パケットをスクリーニングするシステムを提供する。

【解決手段】　このシステムは、プライベート・ネットワークおよび公衆ネットワークのそれぞれに接続され、プライベート・ネットワーク上にあるホストおよびサービスのサブセットをミラーリングすることができる所定の数のホストおよびサービスを含む代行ネットワークに接続された複数（特に３つ）のタイプのネットワーク・ポートを有する専用コンピュータを備える。代行ネットワークはプライベート・ネットワークから分離されており、したがって侵入者の出発点として使用することができない。



1

【特許請求の範囲】

【請求項１】　第１のコンピュータ・ネットワークと第２のコンピュータ・ネットワークの間に接続されたスクリーン・システムに着信したデータ・パケットをスクリーニングし、スクリーン・システムに接続された代行システムで処置を実行する方法であって、

（１）第１のネットワークから第２のネットワークに向けて送られた第１の前記パケットを現行パケットとして受信するステップと、

（２）現行パケットの内容から現行パケットが第２のネットワークに渡すことを許可される所定のタイプのパケットであるか否かを判断するステップと、

（３）ステップ（２）の判断が肯定の場合、現行パケットによって指定された第２のネットワーク内の宛先アドレスを判断し、現行パケットを前記宛先アドレスの代わりとなる代行システム内の代用アドレスに渡すステップと、

（４）現行パケットによって要求された少なくとも１つの処置が許可するようにあらかじめ決められたタイプであるか否かを判断し、そうでない場合には現行パケットを拒否してステップ（６）に進み、そうである場合にはステップ（５）に進むステップと、

（５）現行パケットによって指定された処置をスクリーン・システムと代行システムのうちの少なくとも１つにおいて行うステップと、

（６）他のパケットがスクリーン・システムに着信したか否かを判断し、着信した場合にはそのパケットを現行パケットとして受け取ってステップ（１）に進み、着信していない場合にはこの方法を終了するステップとを含む方法。

【請求項２】　ステップ（５）において、前記宛先アドレスの少なくとも一部を処置の実行場所の唯一の識別子として使用して、代行システムから第１のネットワークに応答データ・パケットを伝送するステップを含む請求項１に記載の方法。

【請求項３】　第１のコンピュータ・ネットワークと第２のコンピュータ・ネットワークに接続され、第１と第２のネットワークの間で伝送されるデータ・パケットをスクリーニングするスクリーン・システムであって、

プロセッサと、

プロセッサに結合されたメモリと、

前記第１と第２のネットワークの間でそれぞれデータ・パケットの送信および受信を行う入力回路および出力回路と、

第１と第の２ネットワークの間のデータ・パケットの流れを制御する前記メモリに記憶されたプログラム命令とを含むシステムであって、

前記プログラム命令は、

第１のネットワークから第２のネットワークに伝送される第１のデータ・パケットが所定の基準を満たしているか否かを判断する第１のプログラム・モジュールと、

所定の基準を満たしている場合には第１のデータ・パケットを第２のネットワークに渡す第２のプログラム・モジュールと、

所定の基準を満たしていない場合には第１のデータ・パケットを第２のネットワークまで通過させないようにする第３のプログラム・モジュールとを備えるシステム。

【請求項４】　第１のコンピュータ・ネットワークと第２のコンピュータ・ネットワークに接続されたスクリーン・システムに着信したデータ・パケットをスクリーニングし、スクリーン・システムに接続された代行システムで処置を実行する方法であって、

（１）第１のネットワークからの第１の前記パケットを第２のネットワークで現行パケットとして受信するステップと、

（２）第１のデータ・パケットの内容から第１のデータ・パケットの要求された操作と送信元アドレスと宛先アドレスとを判断するステップと、

（３）少なくとも１つの所定の基準に基づいて、要求された操作に応答してとる処置を判断するステップと、

（４）代行ホストが代行システムにあり、前記宛先アドレスの代わりとなる代行ホストに現行パケットを渡すステップと、

（５）代行システムにおいて、判断された処置をとるステップとを含む方法。

【請求項５】　少なくとも１つのデータ・パケットが、データ・パケットの意図された受信システムを指定する第１のフィールドを含み、前記意図された受信システムに対して要求された操作を指定する第２のフィールドをさらに含む、第１のコンピュータ・ネットワークと第２のコンピュータ・ネットワークの間に結合され、前記第１のネットワークから前記第２のネットワークに送信された前記データ・パケットをスクリーニングする代行システムであって、

プロセッサと、

前記プロセッサに接続され、前記プロセッサによって実行される操作を指定する命令モジュールを記憶するように構成されたメモリと、

第１のデータ・パケットの内容に関する所定の基準に基づいて、前記スクリーン・システムで受信された少なくとも前記第１の前記データ・パケットについてとるべき所定の１組の処置を指定する命令を含む前記メモリに記憶された複数の処置モジュールと、

前記第１のデータ・パケットの前記第２のコンピュータ・ネットワークへの通過をスクリーン・システムが遮断する命令を含むスクリーニング・モジュールと、

前記要求された操作の代わりに前記代行システム・プロセッサによって行われるべき前記処置のうちの１つを選択するように前記複数の処置モジュールを制御する操作モジュールとを備える代行システム。

【請求項６】　第１のコンピュータ・ネットワークと第２のコンピュータ・ネットワークの間に結合されたスクリーン・システムが攻撃目標となるのを阻止する方法であって、
データ・パケットが第１のネットワークを識別する送信元アドレスと第２のネットワークを識別する宛先アドレスとを含んでいて、スクリーン・システムが、第１のネットワークから第２のネットワークに向けて送られた少なくとも１つの前記データ・パケットを受信するステップと、
所定の基準に基づいてパケットを検査するステップと、
所定の基準が満たされている場合、送信元アドレスと宛先アドレスを変更せずにパケットを第２のネットワークに渡すステップと、
所定の基準が満たされていない場合、パケットを破棄すると同時にスクリーン・システムによる第１のネットワークに対するいかなる応答も阻止するステップとを含む方法。

【請求項７】　第１のコンピュータ・ネットワークと第２のコンピュータ・ネットワークの間に結合されたスクリーン・システムが攻撃目標となるのを阻止する保護システムであって、前記スクリーン・システムが、プロセッサと、そのプロセッサに結合されてプロセッサによって実行可能な命令モジュールを記憶するメモリと、スクリーン・システムを第１のネットワークに結合する第１のネットワーク・インタフェースと、スクリーン・システムを第２のネットワークに結合する第２のネットワーク・インタフェースとを備えていて、前記命令モジュールがデータ・パケットが第１のネットワークを識別する送信元アドレスと第２のネットワークを識別する宛先アドレスとを含み、第１のネットワークから第２のネットワークに向けて送られた少なくとも１つのデータ・パケットを受け取るように構成された第１のモジュールと、
所定の基準に基づいてパケットを検査するように構成された第２のモジュールと、
所定の基準が満たされている場合、送信元アドレスと宛先アドレスを変更せずに第２のネットワークにパケットを渡すように構成された第３のモジュールと、
所定の基準が満たされていない場合、パケットを破棄すると同時にスクリーン・システムによる第１のネットワークに対するいかなる応答も阻止するように構成された第４のモジュールとを備える保護システム。

【請求項８】　第１のコンピュータ・ネットワークが攻撃目標となるのを阻止するシステムであって、
第１のコンピュータ・ネットワークと第２のコンピュータ・ネットワークの間に結合されたスクリーン・システムを有し、そのスクリーン・システムが、プロセッサと、スクリーン・システムを第１のネットワークに結合する第１のネットワーク・インタフェースと、スクリーン・システムを第２のネットワークに結合する第２のネットワーク・インタフェースとを備え、さらに第３のネットワーク・インタフェースを介してスクリーン・システムに結合された代行ネットワークを備え、その代行ネットワークは第１のコンピュータ・ネットワークと共有のドメインを有するインターネットワーク・アドレスを持つ少なくとも１つの代行ホストを備え、
前記スクリーン・システムは、プロセッサによって実行可能な命令モジュールを記憶する、プロセッサに結合されたメモリをさらに備え、その命令モジュールが、
前記ドメインを含む宛先アドレスを含むデータ・パケットを第１のネットワーク・インタフェースを介して受信する第１のモジュールと、
前記宛先アドレスが前記代行ホストに関係する場合、前記代行ホストにデータ・パケットを渡す第２のモジュールとを含むシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、１つのコンピュータ・ネットワークから他のコンピュータ・ネットワークに送信されるデータ・パケットのスクリーニングに関する。テルネット・セッション、ｆｔｐ（ファイル転送プロトコル）セッション、ｅメール（電子メール）など、公衆ネットワーク上のユーザがプライベート・ネットワーク上のホスト機と対話する多くの方法がある。さらに、要求者の端末を直接接続するほかに、所与のターゲット・ネットワーク上のコンピュータがそのネットワークの外部のユーザから特定の操作を実行するように要求されることがある。

【０００２】

【従来の技術】図１に、プライベート・ネットワーク２０、公衆ネットワーク３０、および他のプライベート・ネットワーク４０を含む従来のインターネットワーク１０を図示する。プライベート・ネットワーク２０および４０は、ファイヤーウォールを備えていないときわめて侵入を受けやすくなる。

【０００３】図３に、ネットワーク・インタフェース１６０および１７０を制御する論理（回路、または典型的には関連するメモリを有するプロセッサ）１５０によって制御されるルータまたはブリッジ１３０を介してプライベート・ネットワーク１２０が他のプライベート・ネットワーク１４０と通信することができるインターネットワーク１１０を図示する。ネットワーク１４０から、ホストに宛ててネットワーク１２０上のポートを指定するデータ・パケットが着信すると、そのデータ・パケットはユニット１８０によってそのホストおよびポートに対応づけられ、インタフェース１６０を介してネットワーク１２０上の該当する宛先に送信される。図３では、セキュリティは設けられておらず、したがっていつでも攻撃目標とされる可能性がある。

【０００４】したがって、公衆ネットワーク８０を介し

てプライベート・ネットワーク６０と１００が互いに通信することができるがそれぞれファイヤウォール７０および９０を備える、図２に示すシステム５０におけるようなコンピュータ・ファイヤウォールが開発されている。現在使用されている従来のコンピュータ・ファイヤウォール（および図３のブリッジ１３０のようなルータまたはブリッジ）の問題点は、ファイヤウォールがＩＰ（インターネット・プロトコル）トランザクションに関与し、その際にそれらをＩＰ機として識別する情報を発生し、それによってそれらが侵入者に認識されて攻撃目標となる点である。ファイヤウォールに関するこのタイプおよびその他のタイプの問題の詳細な説明については、たとえば、参照により本明細書に組み込まれるＣｈｅｓｗｉｃｋとＢｅｌｌｏｖｉｎによる参考資料Ｆｉｒｅｗａｌｌｓ ａｎｄ Ｉｎｔｅｒｎｅｔ Ｓｅｃｕｒｉｔｙ（Ａｄｄｉｓｏｎ Ｗｅｓｌｅｙ １９９４）とＳｉｙａｎおよびＨａｒｅによるＩｎｔｅｒｎｅｔ Ｆｉｒｅｗａｌｌｓ ａｎｄ Ｎｅｔｗｏｒｋ Ｓｅｃｕｒｉｔｙ（Ｎｅｗ Ｒｉｄｅｒｓ Ｐｕｂｌｉｓｈｉｎｇ １９９５）を参照されたい。

【０００５】ファイヤウォールおよびパケット・フィルタリング・システムは、攻撃するために用いることができる方法の数を最小限にするように、侵入者にとって認識不能であって、それにもかかわらず適切な機能を満たすのが理想的である。

【０００６】現在のネットワーク・セキュリティ解決策は、ファイヤウォールを設けるほかにネットワークに変更を加える必要があることが多く、複雑で費用が高くつくことがある。ネットワークを実質的に変更することなくネットワークに接続可能であって、保護ネットワークの外部からの侵入に対してはセキュリティを実現するシステムが必要である。

【０００７】通例ルータとして機能し、保護ネットワークに結合された１つのポートまたはネットワーク・インタフェース及び他のネットワークまたはインターネットに結合された他のポートを有するパケット・フィルタリング・システムが、ネットワークにセキュリティを与えるために現在使用されている。ルータとして、このようなシステムはＩＰコマンドに応答し、特にそれらのシステムのＩＰアドレスを使用してデータ・パケットに応答するえあろう。これによって、侵入者はそれらのシステムを識別と攻撃の目標とすることができる。

【０００８】

【発明が解決しようとする課題】保護ネットワーク内のアドレスがそのネットワークの外部のユーザに知られた場合にも、同じタイプの攻撃を受ける。したがって、ネットワーク内のフィルタリング・システムに関するＩＰアドレス情報もホストに関するＩＰアドレス情報も明らかにせずにネットワークの外部からのデータ・パケットに応答することができるシステムを設けると有利である。

【０００９】

【課題を解決するための手段】本発明は、従来の意味でのファイヤウォールとシグネチャレス・パケット・フィルタリング・システムの両方の機能を果たすスクリーン・システムに向けられている。たとえば公衆ネットワークと攻撃目標になることから保護するプライベート・ネットワークとの間のネットワーク接続部にスクリーンを設置する。その２つのネットワークのそれぞれについてポートまたはネットワーク・インタフェースを設け、さらに、１つまたは複数の代行ネットワークに対して１つまたは複数の追加的ポートを設ける。

【００１０】このスクリーン・システムは、各着信パケットを検査してエンジンに送るパケット・フィルタリング・サブシステムまたはモジュールを備え、エンジンはパケット検査機構およびその他の情報に基づいて、そのパケットに対してどのような処置をとるべきかを決定する。パケットは処置サブシステムまたはモジュールに渡され、その処置サブシステムまたはモジュールが適切な処置を実行する。

【００１１】パケットの意図された宛先がプライベート・ネットワーク上のホスト機である場合は、代わりに代行ネットワーク上の事前構成済みホスト機にそらして送ることができ、そのホスト機が、実ホストが実行するはずの適切な操作を実行するか、または所望により異なる操作を実行する。代行ホストは、実ホストのＩＰアドレスを使用して応答を生成するため、代行ネットワークの存在は検知することができない。このスクリーン・システムはルータではなく、したがってそれ自身のＩＰアドレスは持たないため、スクリーン・システムもこのようにして検出することができず、ｔｒａｃｅ＿ｒｏｕｔｅ、ｐｉｎｇ、ｆｉｎｇｅｒなどの操作の対象とならない。

【００１２】このスクリーン・システムは、プライベート・ネットワークまたは公衆ネットワークの変更を必要とせず、ネットワーク接続でインライン接続することができ、所望の数のホストによって代行ネットワークをセット・アップすることができ、それによってプライベート・ネットワークの再構成またはネットワーク・ソフトウェアの変更を行わずにセキュリティが設けられる。

【００１３】このスクリーン・システムは、すべて所定の基準に照らして、エラー・メッセージ付きまたはエラー・メッセージなしでパケットを除去する、パケットを記録する、パケットまたはそのヘッダを変更するなど、パケットに対して広範囲なその他の処置を実行するように事前構成することができる。以上のおよびその他の処置はスクリーン・システムを匿名のままで実行できる。

【００１４】

【発明の実施の形態】

本発明のハードウェア

図４に、本発明の実施に適したインターネットワーク・システムを示す。公衆ネットワーク２００（またはインターネットなど、ネットワークのネットワーク）は、たとえばエンジニアリング・ドメイン・ネットワーク２２０および会社ドメイン・ネットワーク２３０などを含むプライベート・ネットワークまたはインターネットワーク２１０と通信することができる。図のようにネットワーク２２０とネットワーク２３０および２００との間に従来のファイヤウォール２４０を配置する。ファイヤウォールは図のように、所与のプライベート・ネットワーク（２２０）と公衆ネットワーク（２００）との間のほか、プライベート・ネットワーク２００とそのプライベート・ネットワーク自体のプライベート・インターネットワーク上の他のネットワーク（２１０など）との間にも設置することができることに留意されたい。ネットワーク化ハードウェアおよびソフトウェアは、イーサネットなど任意の適合する従来のネットワーク化システムとすることができる。

【００１５】ファイヤウォール２４０は、実施者の所望により、単一の機械として構成することも、一方が着信データ・パケットを処理し他方がネットワーク２２０からの送出データ・パケットを処理する別々の機械として構成することもできる。さらに、会社ドメイン・ネットワーク２３０専用の他のファイヤウォールが通常は使用されることになるが、この図には図示していない。

【００１６】ネットワーク２００または２３０から送信されたデータ・パケットは、接続３００または２８０を介してファイヤウォール２４０に送られる。このファイヤウォール２４０は、以下に記載する点以外は従来通りとすることができる。ファイヤウォール２４０は、許可されたデータ・パケットを接続２５０を介してネットワーク２２０に渡す。

【００１７】同様に、ネットワーク２２０からネットワーク２００内またはネットワーク２３０の宛先に宛てられたデータ・パケットは、接続２７０を介してファイヤウォール２４０に送られ、ファイヤウォール２４０は要求に応じて、セキュリティ条件を条件として接続３１０（ネットワーク２００宛ての場合）または接続２９０（ネットワーク２３０宛ての場合）を介して渡す。接続２５０および２７０～３１０はすべて、たとえばケーブル、光ファイバ、または同様のものなど、従来のネットワーク接続とすることができる。

【００１８】図５は、インターネットワーク・システム３２０で実施することができる本発明のパケット・スクリーン・システム３４０の論理ブロック図である。別法として、このインターネットワーク・システム３２０は図４に示すようなインターネットワークでもよく、したがってファイヤウォール２４０は、従来のファイヤウォール機能のすべてに加えて以下に述べるスクリーニング機能を扱うように構成されたスクリーン・システム３４０に置き換えることができる。

【００１９】図５には、標準ネットワーク・インタフェース４１０を介してパケット・スクリーン・システム（または単に「スクリーン」）３４０に結合された単一のプライベート・ネットワーク３３０が図示されている。さらに、他の標準ネットワーク・インタフェース４２５を介して公衆ネットワーク３５０がスクリーン３４０に結合されている。第３のネットワークである代行ネットワーク４３０が、ネットワーク・インタフェース４２０を介してスクリーン３４０に結合されている。

【００２０】図４および図５に示すようなファイヤウォール接続を使用して、任意の数Ｎのプライベート・ネットワーク（この場合は代行ネットワークを含むものとみなすことができる）を本発明の複数のスクリーン３４０を介して相互に結合することができ、任意の所望の数Ｍの公衆ネットワークに接続することができる。したがって、ＮｘＭのスクリーン・システムを形成することができ、図５の例ではＮ＝２でＭ＝１である。以下の図８Ａの説明も参照されたい。

【００２１】Ｎ＝Ｍ＝１で、データ・パケットを一方向または双方向にＩＰアドレスの変更なしで通過させるか、または何らかの変更を加えるが、スクリーン・システム自体のＩＰアドレスまたはその他のネットワーク・アドレスを追加しない、代行ネットワークのない本発明のシステムも同様に構築することが可能である。このようなシステムについては図８Ｂに関して後述する。

【００２２】図６にユニプロセッサ・ベースまたはマルチプロセッサ・ベースのシステムとすることができるスクリーン３４０を詳細に示す。この実施形態では、本発明によって実行される動作を実行するために必要な命令を記憶する１つまたは複数の従来のメモリ（たとえばＲＡＭ、ＲＯＭ、ＥＰＲＯＭ、ディスク記憶装置など）４００に結合された単一プロセッサ３９０が図示されている。ネットワーク・インタフェース４１０～４２５はプロセッサ３９０によって従来の方式で制御される。

【００２３】プライベート・ネットワークは、典型的には多くの異なるホストを含む。例としては、ｅメール・ホスト３６０、ｆｔｐ接続を管理するｆｔｐ（ファイル転送プロトコル）ホスト３７０、およびWWW（ワールドワイド・ウェッブ）サーバなどのその他サービスのためのホスト３８０、ｒｌｏｇｉｎ（リモート・ログイン）、およびｒｓｈｅｌｌのためのホストなどがある。

【００２４】代行ネットワーク４３０は代行（または仮想）ホスト４３５を含む。代行ホスト４３５は別個のコンピュータ・システムであることが好ましい。好ましい実施形態では、代行ネットワーク４３０は、プライベート・ネットワーク３３０にあるホストのサブセット（またはすべて）のそれぞれを、後述のようにしてミラーリング（すなわちその代行として機能する）仮想ホストを備える。

【００２５】この実施形態では、二重化したい各実ホストについて１つずつの仮想（代行）ホスト、すなわち、代行メール・サーバ４４０、代行ｆｔｐサーバ４５０、およびその他の仮想ホスト４６０を含む上記のような仮想ホストが示されている。二重化する各実ホストには、実ホストのうちの一部または全部を含めることができる。代行ホストは、実際のターゲット・ホスト３６０～３８０ではなくそれらのホストの動作を模倣するという意味で「仮想」である。しかし、代行ホストは代行ネットワークにおいては実際のハードウェアまたはソフトウェアあるいはその両方である。

【００２６】代行ネットワークに固有のホストも含めることができる。たとえば、代行ネットワーク４３０は、代行サーバに固有の、すなわち、単なるネットワーク３３０内のWWWサーバのミラーまたは代行ではないWWWサーバ４４５を含むことができる。この場合、ネットワーク３５０からユーザが、http://www.<private.network>.comへの接続を要求すると、そのユーザはWWWサーバ４４５に接続される。代行ネットワーク４３０に固有の他のサーバ４５５も設けることができる。

【００２７】したがって、代行ネットワークは、実ホストを表す代行ホスト、または固有サーバを有する代行ホスト、あるいはその両方を、任意の組合せ（それぞれゼロから数個まで）で含むことができる。いずれの構成を採用する場合も、プライベート・ネットワーク３３０と代行ネットワーク４３０が合わさって単一の論理ネットワークまたは見かけのネットワーク３４５、すなわち、公衆ネットワーク３５０上のユーザなど部外者の視点から見て単一の見かけのドメインを形成し、ユーザがプライベート・ネットワークのサービスまたはホストにアクセスしようと試みた場合、その要求を代行ネットワークの方にそらしてミラリング代行ホストまたは固有代行ホストに送ることができ、その際そのユーザにはこれが行われたということをまったく示さない。「代行ホスト」とは、実ホストの代行を意味することも、固有ホストであるにもかかわらず代行ネットワーク上のホストであることを意味する場合もあることに留意されたい。

【００２８】図７に、本発明のシステムの代替実施形態、すなわち、代行ネットワーク４３０全体がスクリーン３４０のメモリ４００に記憶されているプログラム命令で実施されるか、または１つまたは複数のメモリに記憶されているプログラム命令によって制御される追加のプロセッサおよびメモリとして実施されているシステム３２５を示す。この場合、図６に示すスクリーン３４０と代行ネットワーク４３０は、別々の論理実体を構成するが、別々の物理実体ではない（ただし、命令、データ、コマンド、信号など自体は別々の物理実体ではある）。つまり、スクリーン３４０と代行ネットワークは単一のユニットであることができる。この実施形態では、代行ホスト３６０～３８０はプログラム命令によってエミュレートされ、いずれの実ホストの動作も、仮想代行ホスト・モジュールによって模倣することができる。本開示の残りの部分では図５～図６を参照するが、図７の実施形態にも同様に適用されるものと理解されたい。

【００２９】図８Ａは、図５～図６に示すスクリーン３４０を詳細に示した、本発明のシステムを実施するハードウェアのブロック図である。図中の同様の番号が付いた要素は同様のものである。したがって、図８Ａにはさらに従来のディスク記憶装置５００と、スマート・カード、キーボード、マウス、モニタ、その他の標準Ｉ／Ｏ装置などのＩ／Ｏ（入出力）装置５１０、ならびに所望のその他の従来の記憶装置またはメモリ５２０が追加されて備えている様子が図示されているのがわかるであろう。メモリ４００に記憶されている命令またはプログラム・モジュールが、スクリーン３４０の動作を制御する。

【００３０】１つの実施形態では、スクリーンは従来のユーザ・レベルのアクセスを行えない、すなわち、標準キーボードやモニタを備えない。これは、スクリーンの構成に改変が加えられるのを防止するセキュリティ機能である。このような実施形態では、スクリーンは、認証され、暗号化され、専用の特殊目的管理プロトコルに従った通信に対してのみ応答する、秘密ＩＰ（またはその他のプロトコル）アドレスを持つ専用ネットワーク・ポートを介して遠隔管理される。このようなプロトコルと、使用する暗号化方式、および認証方式は、スクリーン管理者が開発または選定、あるいはその両方を行う。

【００３１】図８Ａに示すように、スクリーン３４０は、公衆ネットワークに接続された（図５のような）単一ポート４２５の代わりに、複数ポート４２７を備える複数の公衆ネットワークにそれぞれ接続するとができ、他のプライベート・ネットワーク３３５に接続された１つまたは複数の追加ポート４１５を備えることもできる。たとえば、プライベート・ネットワーク３３５を１つの会社内のエンジニアリング・ドメインｅｎｇ．ｓｕｎ．ｃｏｍとすることができ、プライベート・ネットワーク３３０を同じ会社内の会社ドメインｃｏｒｐ．ｓｕｎ．ｃｏｍとすることができる。ｅｎｇ．ｓｕｎ．ｃｏｍドメインとｃｏｒｐ．ｓｕｎ．ｃｏｍドメインは、接続３３７を介して相互に（所望の場合は、図示されていない追加の本発明のスクリーンをまたは従来のファイヤウォールを通して）通信することができ、単一のプライベート・インターネットワーク３５５を形成すると同時に、これらのドメインは両方ともスクリーン３４０によって公衆ネットワーク３５０からの侵入から保護される。この実施形態の代行ネットワーク４３０は、ｅｎｇ．ｓｕｎ．ｃｏｍドメインとｃｏｒｐ．ｓｕｎ．ｃｏｍドメインの両方の代行を備える。

【００３２】したがって、本明細書の説明の以下で述べ

る通信は、単一の公衆ネットワーク３５０と単一のプライベート・ネットワーク３３０の間で行われるものと仮定するが、本発明の特徴は、スクリーン３４０を介して複数の公衆ネットワーク３５０に接続された複数のプライベート・ネットワーク３３０、３３５にも等しく適用可能である。

【００３３】図８Ｂに示すシステム５３０では、プライベート・ネットワーク５４０は本発明にクリーン・システム５４０が設けられているが、代行ネットワークはない。この実施形態および他の実施形態では、データ・パケットはいずれの方向にも、それぞれのＩＰアドレスの変更なしで、あるいは何らかの変更は行われるがスクリーン・システム自体のＩＰアドレスまたはその他のネットワーク・アドレスを追加せずに送信される。アドレスを変更するか否かの決定は、所定の基準に従ってパケットごとに行うことができる。

【００３４】したがって、本発明のシステム（５～９の実施形態のいずれをも含む）では、パケットとともに提供される送信元アドレスと宛先アドレスは、（変更されるか否かを問わず）そのパケットに関連する唯一のホスト識別子またはアドレスのままとなる。この実施形態の代替案では、スクリーン・システムは送信元アドレスまたは宛先アドレス（あるいはその両方）の代わりに他のネットワーク・アドレスを用いることができ、その場合、新たに代用されたアドレスは、偽であるかまたはスクリーン・システム以外のホストのものである。いずれの場合も、データ・パケットには、スクリーン・システムに関係するネットワーク・アドレスは付加されない。

【００３５】前述のように、スクリーン・システムはＩＰアドレスまたはその他のネットワーク・アドレスすらも持たないことが好ましく、ＩＰプロトコルを「解釈」することはできるが、ＩＰ要求に応答しないように構成される。

【００３６】以下に、図５～図６のシステムの動作について図９～図１１に関連して詳述するが、本発明の他の実施形態にも適用されるものと理解されたい。上記および以下で述べている本発明のシステムによって実行される動作、処置、または機能のそれぞれは、プログラム命令またはモジュール、ハードウェア（たとえばＡＳＩＣまたはその他の回路、ＲＯＭなど）、またはそれらの何らかの組合せとして実施することができる。

【００３７】データ・パケットの一般的処理

図６で、公衆ネットワーク３５０からホストまたはサーバ３６０～３８０のうちの１つに宛てられたデータ・パケットが着信すると、スクリーン３４０によってインタセプトされる。このようなパケットは一般に送信元アドレス、宛先アドレス、要求操作またはサービスあるいはその両方、およびメッセージ（電子メールの場合）、操作対象データなどのその他の情報が含まれている。

【００３８】スクリーン３４０は、着信（および送出）データ・パケットに対して取る処置の制御を司る命令をメモリ４００に記憶している。これらの命令は、データ・パケットの前記の内容（送信元アドレスおよび宛先アドレス、サービスのタイプ、またはデータ・パケットから入手可能なその他の情報）と、パケットの送信時刻またはスクリーンによる受信時刻、公衆ネットワークとプライベート・ネットワークの間の接続状態（またはプライベート・ネットワーク内の特定のホストまたはサービスとの接続状態）、および送信元アドレスが予期された（インター）ネットワーク場所から出たものであるか否かなどのより間接的に入手可能な情報などその他の情報とに基づく所定の１組の基準を含む。これは、送信元ホストが予期されたドメイン内にあるか否かを判断することによって行うか、またはパケットがそのパケットのために予期されていたネットワーク・インタフェースに着信したか否かを判断することによって行うことができる。たとえば、送信元アドレスがプライベート・ネットワーク３３０上のホストであると識別されたパケットは、公衆ネットワーク３５０用のネットワーク・インタフェース４２５（図６）に着信してはならない。着信する場合は、侵入者がトラステッド・ホストを装ってそのプライベート・ネットワークに侵入しようとしている可能性があるという標識である。その場合、スクリーン３４０は応答せずにパケットを除去しなければならない。

【００３９】このようなスクリーニング基準は、データ・パケットの内容の検査、外部データ（接続状況および時刻など）の参照、および所定のテーブルまたは基準を実現するのに有用なその他の情報の参照によって実現することができ、メモリ４００に記憶することができる。たとえば、使用が許可されている操作およびサービスのタイプと相関するネットワーク３３０と通信することが許可されているすべての送信元アドレス、接続またはパケットの受け渡しが許可された時刻、送信元のために予期されている場所（予期されていない送信元からの接続はセキュリティ問題を示している可能性があるため）、送信元がトランザクションの開始を許可されている回数、特定の送信元がネットワーク３３０のサービスの使用を許可されている（たとえば１日または１月当たりの）合計時間などのテーブルを設けることができる。

【００４０】このスクリーニング基準の適用によって、スクリーン３４０は各データ・パケットに対して１つまたは複数の事前定義された処置をとることになる。以下に、これらの処置について述べる。

【００４１】パケットに対してとる処置

スクリーン・システム３４０は、前述の基準と、特定のセキュリティ・プロトコル、およびシステム管理者によってあらかじめ決められた当該パケットのレベルに基づいて、各データ・パケットに対する処置をとる。たとえば、あらかじめ許可されていない送信元からの（またはそのような送信元への）パケットは通過させないことに

することができる。その場合、他の送信元からの（または他の送信元への）パケットは、それ以上の処置を行わずにスクリーン３４０によって除去され、その際、エラー・メッセージまたはその他の通信を送信側に戻す場合も戻さない場合もある。送信側にはパケットに何が起こったのかは示されず、「偽の」メッセージも出さない。

【００４２】これによってシステムに対する攻撃が防止される。たとえば、パケットに応答する正規のＩＰ手続きに従わずにｔｒａｃｅ＿ｒｏｕｔｅパケットを受信した場合、本発明のスクリーンはそれを単に破棄するだけであり、このようにしてｔｒａｃｅ＿ｒｏｕｔｅコマンドの発行者はスクリーンを検知することができない。

【００４３】トポロジ隠蔽、すなわちパケットがスクリーンを通過したときのパケットのネットワーク・アドレスの変更を行って、パケットが多数の送信元から送られた場合であっても、スクリーンから出たパケットがすべて同じホストから送られたように見えるようにすることができる。これにより、部外者がプライベート・ネットワーク内のユーザＩＤ、ホスト名などを知ることによって入手することができる知識を利用しようとする試みが阻止される。

【００４４】他の処置は、当然、単にパケットを通過させてその宛先に渡すことであり、その際、所定の基準に基づいて何らかの変更を行う場合も行わない場合もある。たとえば、プライベート・ネットワーク３３０内の所与のホストから送られたすべてのパケットがユーザＩＤまたはホストＩＤが除去されているようにし、パケットが他の何らかのＩＰ送信元アドレスを付けて渡されるように、前もって決めることができる。

【００４５】システム管理者によって定義された基準に従って、特定のデータ・パケットについて暗号化と暗号解読を自動的に行うこともできる。これに加えて、参照により本明細書に組み込まれる１９９４年９月１５日出願のＳｙｓｔｅｍ ｆｏｒＳｉｇｎａｔｕｒｅｌｅｓｓ Ｔｒａｎｓｍｉｓｓｉｏｎ ａｎｄ Ｒｅｃｅｉｐｔｉｏｎ ｏｆ Ｄａｔａ Ｐａｃｋｅｔｓ Ｂｅｔｗｅｅｎ Ｃｏｍｐｕｔｅｒ Ｎｅｔｗｏｒｋｓという名称の出願人の同時係属の米国特許出願第０８／３０６３３７号の事例で述べられているように、パケットをカプセル化し、パケットに新しいＩＰアドレスが入った新しいヘッダを付けることが望ましい。

【００４６】パケットは、時刻、送信元および宛先のアドレス、要求された操作、各パケットに対してとられたその他の処置、当該送信元からそれまでに送られた要求の数など、システム管理者が重要であると決めた任意の情報を含めて（特に失敗した試行または要求）、通常ログ・ファイル記憶域６４０に記録される。

【００４７】パケット数をカウントし、それによって特定の期間に処理された現在合計数を記録することもできる。

【００４８】上記でアドレス書き換えについて述べた。パケットによって搬送されるデータまたはメッセージの書き換えまたはその他の方法による変更など所定の処置によって、パケットの他の内容も自動的に書き換えることができる。

【００４９】パケットに関する状態情報も、処置によって判断し、所望であれば記録し、変更することができる。たとえば、所望に応じてＴＣＰ／ＩＰ（伝送制御プロトコル／インターネット・プロトコル）状況を変更して接続の確立、維持、または終了を行うことができる。一般に、スクリーンは、各パケットがどのような状態にあるかに関する情報を記憶し、どのパケットが初期要求だったか、応答はどれであるかなどに関する情報の維持を含む、その状態に応じた処置をとることができる。したがって、以前の事象を一定期間のあいだ記憶していなければならないことがあるが、その場合はスクリーンが一連のトランザクションの全履歴を判断し、その都度適切な処置をとることができる。

【００５０】セキュリティのための重要な処置は、あたかも代行ホストが実際の意図された宛先サーバであるかのようにパケットに対して操作を実行する前述のようなサーバ／ホストを備えた代行ネットワーク４３０に、パケットをそらして送信する処置である。このような操作の実行時、代行ホストは所与のパケットを送信側に戻すこと、すなわち元の送信側アドレスを宛先としてパケットを送信することができる。そのパケットは次にスクリーン３４０を通り、スクリーン３４０は、たとえば公衆ネットワーク３５０から、スクリーンで最初に受け取ったときと同じように、パケットを所定の検査基準にかける。この基準は一般に、代行ネットワーク４３０またはプライベート・ネットワーク３３０から送られたパケットについて異なる結果をもたらす。たとえば、公衆ネットワークの外部のホストはプライベート・ネットワークとのテルネット・セッションを確立することができないが、プライベート・ネットワーク内のホストはプライベート・ネットワークの外部のホストとのテルネット・セッションを確立することが「できる」ものと決めることができる。

【００５１】スクリーン・システムは（ＩＰまたはその他の）ネットワーク・アドレスを持たないことによって、そのセキュリティ機能を匿名で実行することができ、特に、従来のネットワーク・ブリッジとして機能しない。スクリーン３４０がブリッジの機能を備えているとすれば、ＩＰコマンドに応答しなければならないことになり、したがって検知可能となり攻撃目標となる。

【００５２】代行ネットワークはさらに、部外者が決して実際にプライベート・ネットワーク３３０に侵入できないようにするという利点を有する。ユーザがいったんプライベート・ネットワークへのアクセスまたは接続を許可されると、アクセスがまったく許可されない場合と

比較して、そのユーザのアクションを制限することははるかに困難になる。代行ネットワーク内のプライベート・ネットワークのサービスの一部の、複製またはミラーリングされた機能、または、代行ネットワーク内の固有ホストまたはその他のサービス（ハードウェアまたはソフトウェア、あるいはその両方）の機能、あるいはその両方によって、外部ユーザの要求が満たされると同時に、そのユーザが実際にプライベート・ネットワークにアクセスするのを、見えない方式で防ぐ。

【００５３】さらに、代行パケットはシステムによる「信用度」が高いため、代行ネットワークからのパケットはスクリーンによる再送信のために乗り越えなければならないハードルが一般に低くなるので、プライベート・ネットワークのセキュリティを危険にさらす可能性があるセッションを代行ネットワークからはまったく確立できないようにすることもできる。代行ネットワークがＴＣＰセッションを開始することができるようにすると、システムの外部からの侵入者は、公衆ネットワークからセッションを開始しなくても、代行ネットワークにＴＣＰセッションを開始させる方法を見つけ出すことができた場合、ファイヤウォール・セキュリティを事実上迂回することができる。

【００５４】プライベート・ネットワーク「から」公衆ネットワーク「への」特定の接続を確立することができるようにし、その逆はできないようにすることが望ましい場合がある。たとえば、公衆ネットワーク３５０へのＴＣＰセッション（テルネットまたはｆｔｐなど）は、プライベート・ネットワーク３３０内のユーザによっては開始することができるが、公衆ネットワークからプライベート・ネットワークへは遮断される。

【００５５】一般に、代行ネットワークによって行われるすべての処置は、代行ネットワークまたはその中のホストを別個のＩＰ実体として識別することなく、パケットを受け渡しする。したがって、パケットは処理後に受け渡しされるか戻されると、指定された宛先ホストによって実際に処理されたように見えるか（実際に代行ホストがそれを処理した場合）、または宛先アドレス（戻りパケットの送信元アドレス）を除去、変更またはその他の方法でわからないようにするように処理される。いずれの場合も、代行ホスト用のＩＰアドレスは存在せず、いかなるパケットに追加されることもない。

【００５６】スクリーン・システムの機能アーキテクチャ

図９は、図８に対応する機能ブロック図であるが、スクリーン３４０によって使用される機能モジュールが示されている。好ましい実施形態では、これらのモジュールは、前記のように、メモリ４００に記憶されていてプロセッサ３９０によって実行されるプログラム命令モジュールである。

【００５７】図９に示すモジュールは、各ネットワーク

・インタフェース４１０～４２５用のプロセス６０２～６０６を有するパケット検査機能６００と、規則６２０を有するエンジンと６１０と、処置６３０およびログ・ファイル記憶域６４０と、従来のハッシュ・テーブルであるパケット状態テーブル６５０と、キャッシュ分割モジュール６７０（図のような分割迂回路を有する）と、各ネットワーク・インタフェース４１０～４２５に結合されたパケット分割機能６６０と、学習ブリッジ・テーブル６８０とを含む。図９に示す接続は、本発明の特定の物理的実施態様に応じて、論理（ソフトウェア）命令またはハードウェア命令、あるいはその両方を指す。

【００５８】パケット検査機能６００は、前述の基準に基づいて着信パケットの内容を検査する命令を備える。つまり、どこからであっても着信データ・パケットが送られてくると、各着信パケットはパケット検査機能６００によるパケット検査を受ける。

【００５９】エンジン６１０が着信パケットを処理して処置６３０に渡し、前述のようにそれらのパケットに対して適切な操作が行われる。処置モジュール６３０は、これらの操作の実行専用のモジュールである。

【００６０】ログ・ファイル記憶域６４０を使用して、前述のように、スクリーン３４０で受信されたデータ・パケットに関する情報が記憶される。同時にパケット状態テーブル６５０を使用して、受信パケットの状態に関する情報が記憶される。

【００６１】分割機能６６０は従来の方式で機能して所定の最大伝送単位（ＭＴＵ）より大きいパケットを分割する。これは、たとえばスクリーンがパケットに情報を追加してその大きさがこの許容最大サイズを超える大きさにした場合に起こることがある。分割キャッシュ６７０を従来の方式で使用してパケットの分割と再構成を行う。一般に分割パケットは、主にまたは単にＩＰヘッダ情報とデータのみを含み（特に、ポート番号は含まれない）、スクリーン３４０は分割キャッシュを使用してパケットを必要に応じて再構築する。つまり、最初の分割パケットが分割キャッシュに記憶され、それ以降の分割パケットも同様に記憶されて、最後の分割パケットを受信してから、そのパケットが再構成される。

【００６２】分割迂回路６７５は、分割キャッシュ６７０内で情報が見つかった分割パケットのエンジン操作をパケット検査機能が迂回するために使用される。したがって、一連の分割パケットの中の２番目以降の分割パケットを受信すると、そのことはパケット検査機能６００が分割キャッシュ６７０を調べたときに検出される。その場合、新たに受信した分割パケットは、エンジン６１０を介さずに迂回路６７５を介して処置６３０に送られる。

【００６３】学習ブリッジ・テーブル６８０によって、スクリーン３４０は従来の学習ブリッジとして機能することができる。すなわち、どのホストがスクリーンのど

ちら側にあるかを追跡し、スクリーンのポート（ネットワーク・インタフェース）のそれぞれに一方のホストまたは他方のホストからパケットが着信すると、この情報のテーブルのメンテナンスを行う。

【００６４】スクリーン・システムの動作

図１０～図１１は、本発明の方法の好ましい実施形態を示すフロー・チャートである。たとえば公衆ネットワーク３５０のホストによってパケットが送られると、そのパケットはスクリーン３４０のポート（インタフェース）４２５で受けられる。図１０のボックス８００を参照されたい。パケット検査機能が前述のようにパケットの内容を検査する（ボックス８１０）。

【００６５】パケットを拒否する場合、（送信元アドレスの）学習ブリッジ・テーブル６８０を使用してそれを行うと効率的である。

【００６６】パケット検査を実施するのに適した１つの実施形態を、図１１のフロー・チャートに示すが、多くの変更態様が可能である。この例示のフロー・チャートでは、パケットを受け取ると（ボックス９００）、各パケット・ヘッダが順に検査される（ボックス９１０）。すなわち、物理リンク（ＩＰなど）、ＩＰヘッダ（ＴＣＰか否か）、ＴＣＰヘッダ（どのポートが指定されているか、および既存の接続か新規の接続かに関して）などが検査される。

【００６７】ボックス９２０および９４０で、否定の判断であればボックス９３０に進んで適切な処置がとられる。肯定の判断であればボックス９５０に進み、指定されているポートが判断され、ボックス９６０に進み、ヘッダ情報のほか、パケットの内容、送信元、宛先、および前述のその他の情報など、パケット検査機能が自由に使える情報を考慮して、その特定の接続が許可されるか否かが判断される。

【００６８】その接続が許可されない場合は遮断されるが（ボックス９７０）、許可される場合は、この方法はそれが初期接続であるか否かを調べる（ボックス９８０）。初期接続の場合は、ボックス９９０でその接続が確立され、ボックス９９５で状態テーブル６５０（図９参照）に情報が格納されて、その新しい接続が識別される。初期接続でない場合は、ボックス１０１０で接続が検査され、更新情報（たとえば接続に関する新しい情報）があればそれがテーブル６５０に格納される。

【００６９】この方法は、ステップ９９０または１０２０からボックス１０００に進む。すなわち図１０のボックス８１０に戻る。

【００７０】前述のように図１１は、パケット検査段階で行うことができる多くの可能な検査および操作の順序の、１つの実施形態に過ぎないことが理解されよう。図１１で実行される動作は、（たとえばボックス９２０、９４０、９６０、および９８０での）パケット検査の結果に基づいてエンジン６００によって行われる。

【００７１】図１０のボックス８２０に進んで、パケットはエンジン６１０に渡され、エンジン６１０は前述の事前定義された適切な操作を実行する。一般に、ファイヤウォール／スクリーン３４０の場合、これにはパケットの遮断または通過が伴い、通過させる場合にはパケットは代行ネットワーク４３０内の代行ホストによって操作されるようにそらすことができる。

【００７２】したがって、現行パケットは適切な処置の実行のために処置モジュール６３０に渡され（ボックス８３０）、ボックス８４０でエンジンは、パケット検査機能の結果とどの処置をとるのが適切であったかというエンジン自身の判断とに基づいて、とるべき処置が他にないかどうかを判断する。所与のパケットの最初の通過時には、（たとえばパケットを除去してそれ以上の処置を行わない場合などそれが「唯一の」処置である場合であっても）取るべき処置が少なくとも１つあることになり、したがって最初の通過時にはボックス８４０からボックス８５０に進み、最初の処置がとられる。

【００７３】この方法は次にボックス８３０に戻り、このループはエンジンによって判断されたすべての処置が処置モジュールによって行われると完了する。その時点で、ボックス８４０の次にボックス８６０に進み、スクリーン３４０が、入力ポート（ネットワーク・インタフェース）の１つに他のパケットがあるか否かを判断する。ある場合には、この方法はボックス８００で新たに開始し、ない場合にはこの方法はボックス８７０で終了する。新しいパケットを受信するといつでも再び開始することができる。

【図面の簡単な説明】

【図１】　２つのコンピュータ・ネットワークを公衆ネットワークを介して接続するシステムのブロック図である。

【図２】　介在ファイヤウォールを使用して、２つのコンピュータ・ネットワークを公衆ネットワークを介して接続するシステムのブロック図である。

【図３】　２つのコンピュータ・ネットワーク間にブリッジを備える従来のシステムを示す図である。

【図４】　ファイヤウォールを介した、プライベート・ネットワークおよび公衆ネットワークから他のプライベート・ネットワークへの接続例を示すブロック図である。

【図５】　本発明によるパケット・スクリーン・システムを備えるコンピュータ・インターネットワークのブロック図である。

【図６】　インターネットワーク上の本発明のパケット・スクリーン・システムを示す機能ブロック図である。

【図７】　本発明のパケット・スクリーン・システムの代替実施形態を示すブロック図である。

【図８】　本発明を実施するハードウェアのブロック図である。

19　　20

【図９】　本発明の機能ブロック図である。

【図１０】　本発明の好ましい実施形態によるパケット・スクリーニングの方法を示すフロー・チャートである。

【図１１】　本発明の好ましい実施形態によるパケット・スクリーニングの方法を示すフロー・チャートである。

【符号の説明】

３２０　インターネットワーク・システム

３３０　プライベート・ネットワーク

３４０　スクリーン・システム

３４５　論理ネットワーク

３５０　公衆ネットワーク

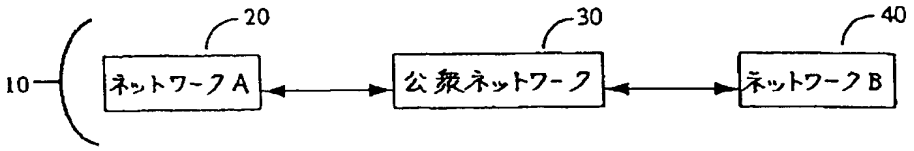
４１０　ネットワーク・インタフェース

４２０　ネットワーク・インタフェース

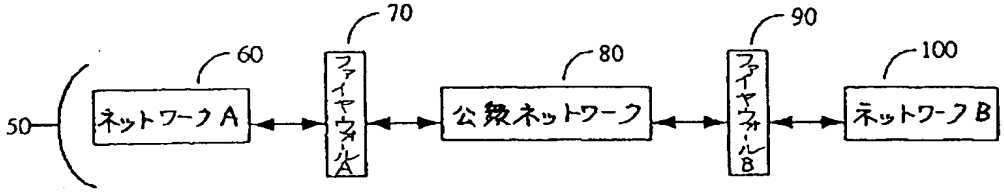
４２５　ネットワーク・インタフェース

４３０　代行ネットワーク

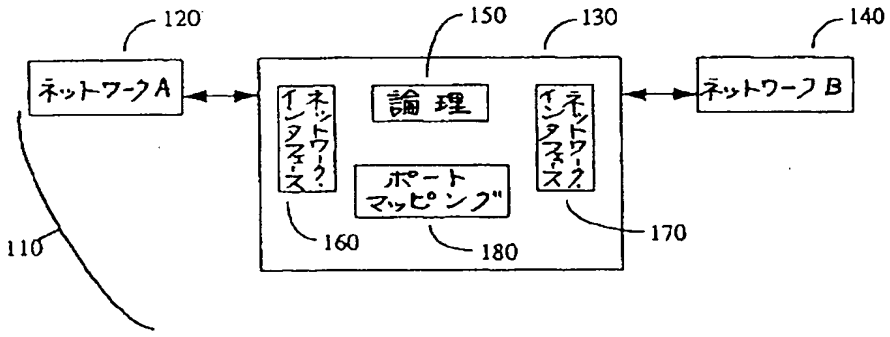
【図１】



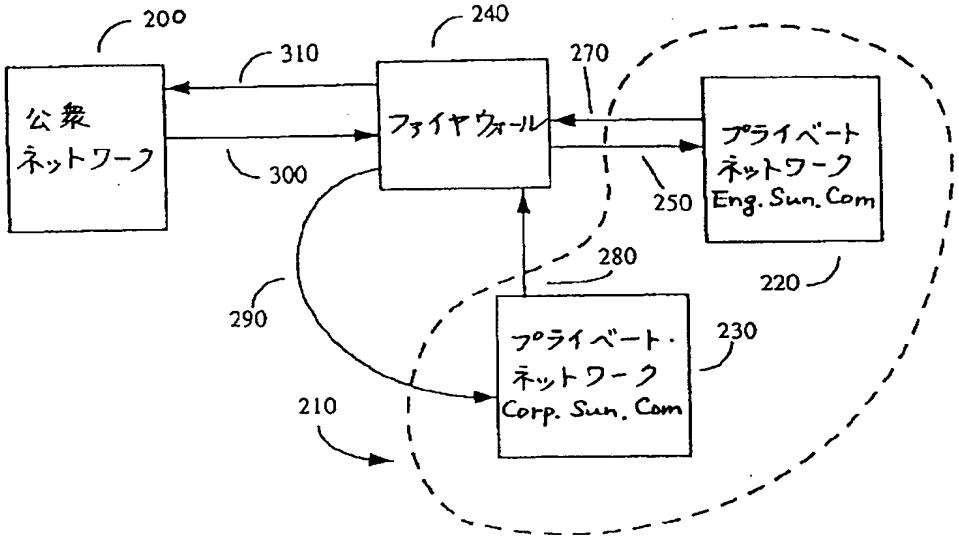
【図２】



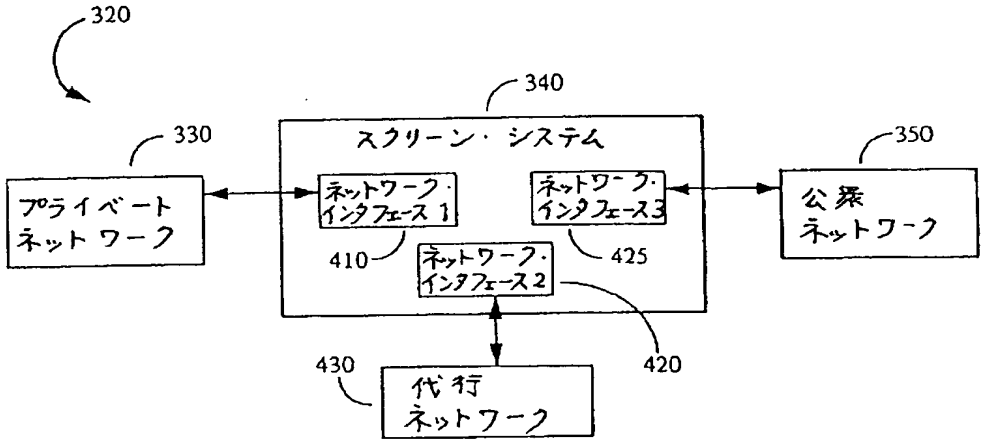
【図３】



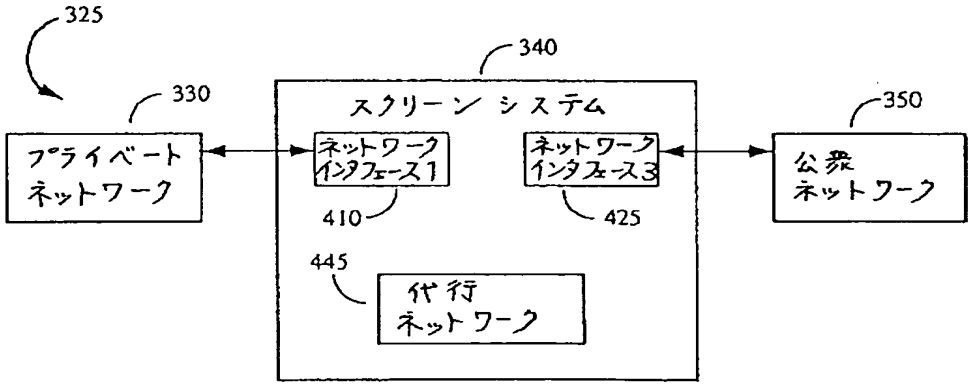
【図４】


200
240
310
270
公衆
ネットワーク
ファイヤウォール
プライベート
ネットワーク
Eng. Sun. Com
300
250
280
220
290
プライベート・
ネットワーク
Corp. Sun. Com
230
210

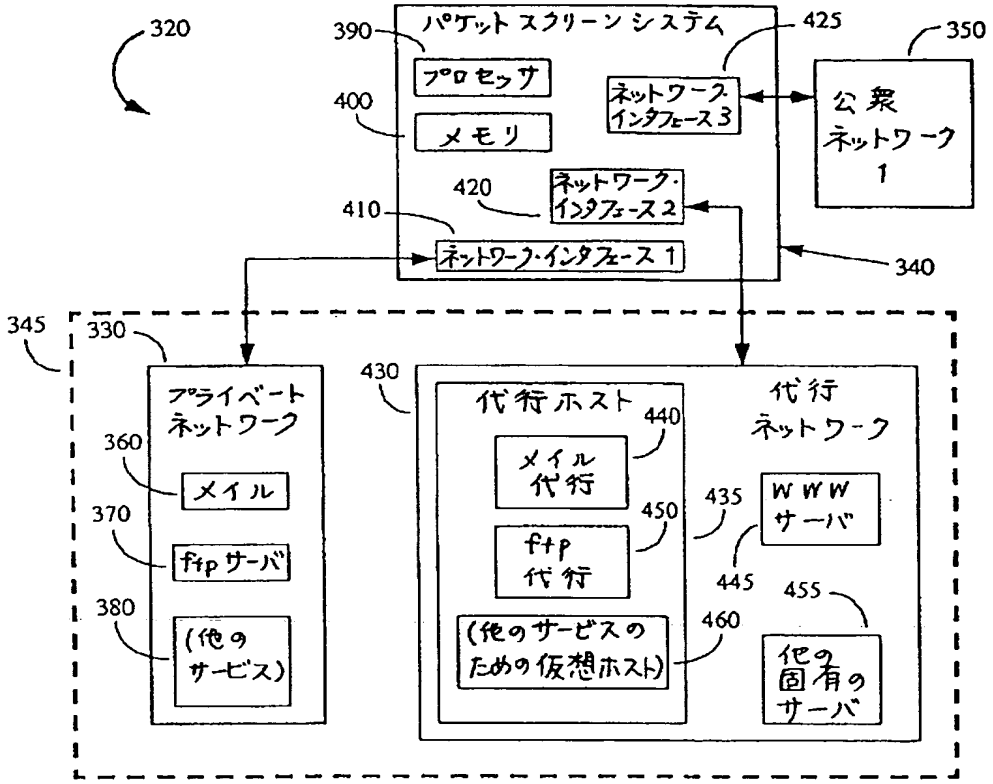
【図５】


320
340
330
スクリーン・システム
350
プライベート
ネットワーク
ネットワーク・
インタフェース1
ネットワーク・
インタフェース3
公衆
ネットワーク
410
425
ネットワーク・
インタフェース2
420
430
代行
ネットワーク

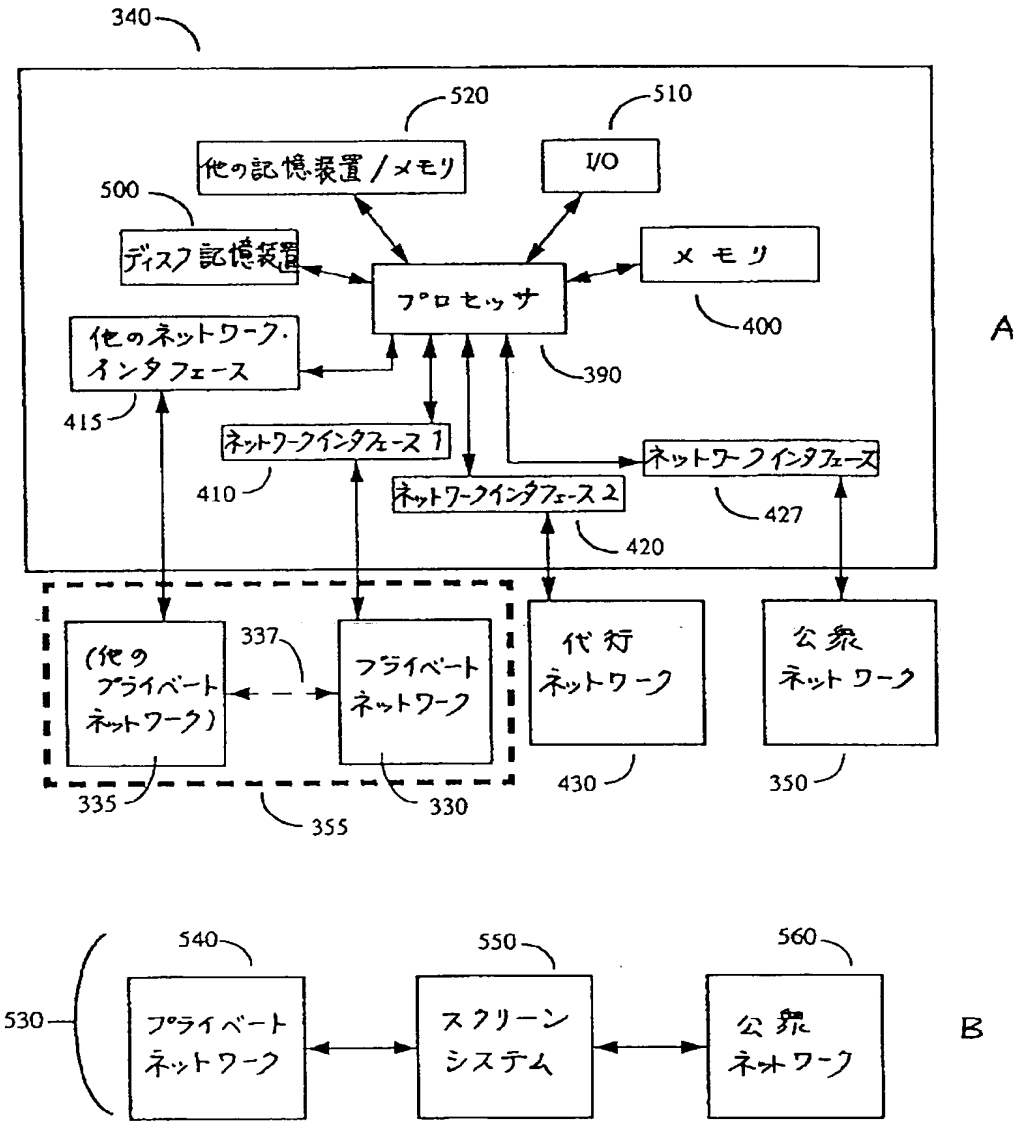
【図７】


325
340
330
スクリーン システム
350
プライベート
ネットワーク
ネットワーク
インタフェース1
ネットワーク
インタフェース3
公衆
ネットワーク
410
425
445
代行
ネットワーク

【図６】

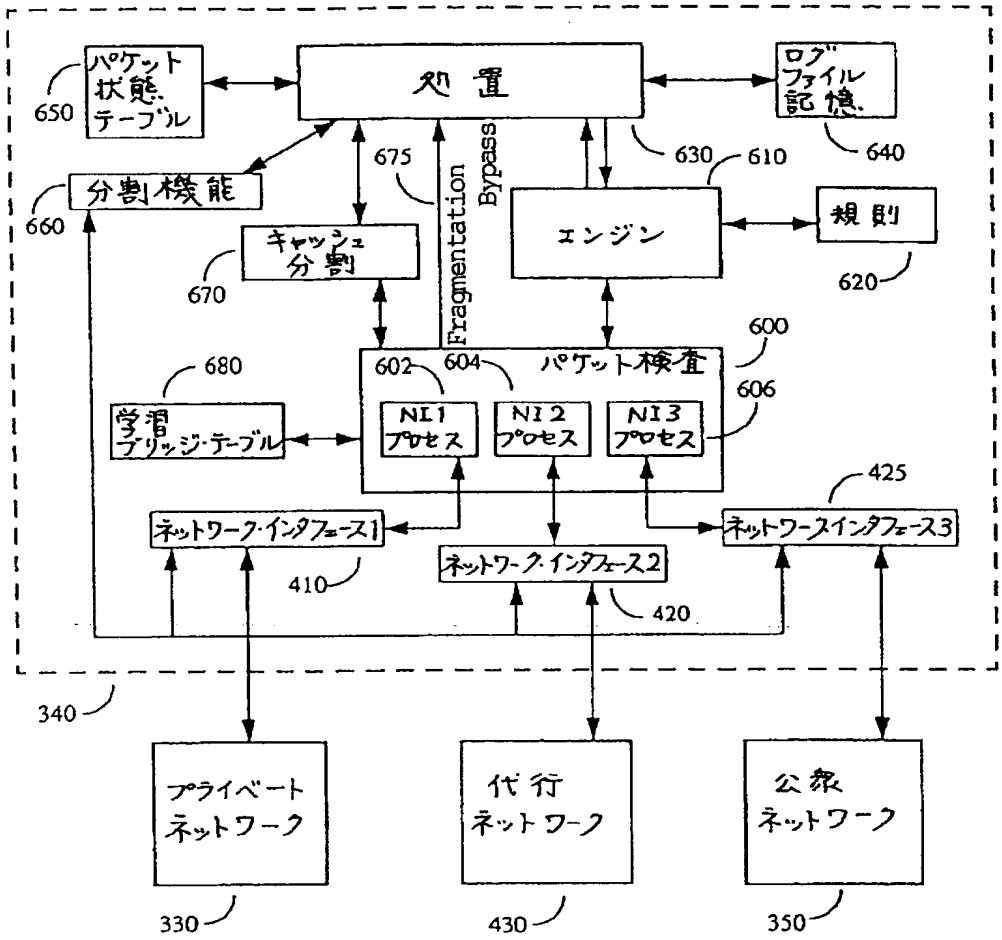

320
パケット スクリーン システム
390
プロセッサ
400
メモリ
425
ネットワーク インタフェース3
350
公衆 ネットワーク 1
420
ネットワーク・インタフェース2
410
ネットワーク・インタフェース1
340
345
330
プライベート ネットワーク
360
メイル
370
ftpサーバ
380
(他の サービス)
430
代行ホスト
440
メイル 代行
450
ftp 代行
(他のサービスの ための仮想ホスト)
代行 ネットワーク
435
WWW サーバ
445
455
460
他の 固有の サーバ

【図８】

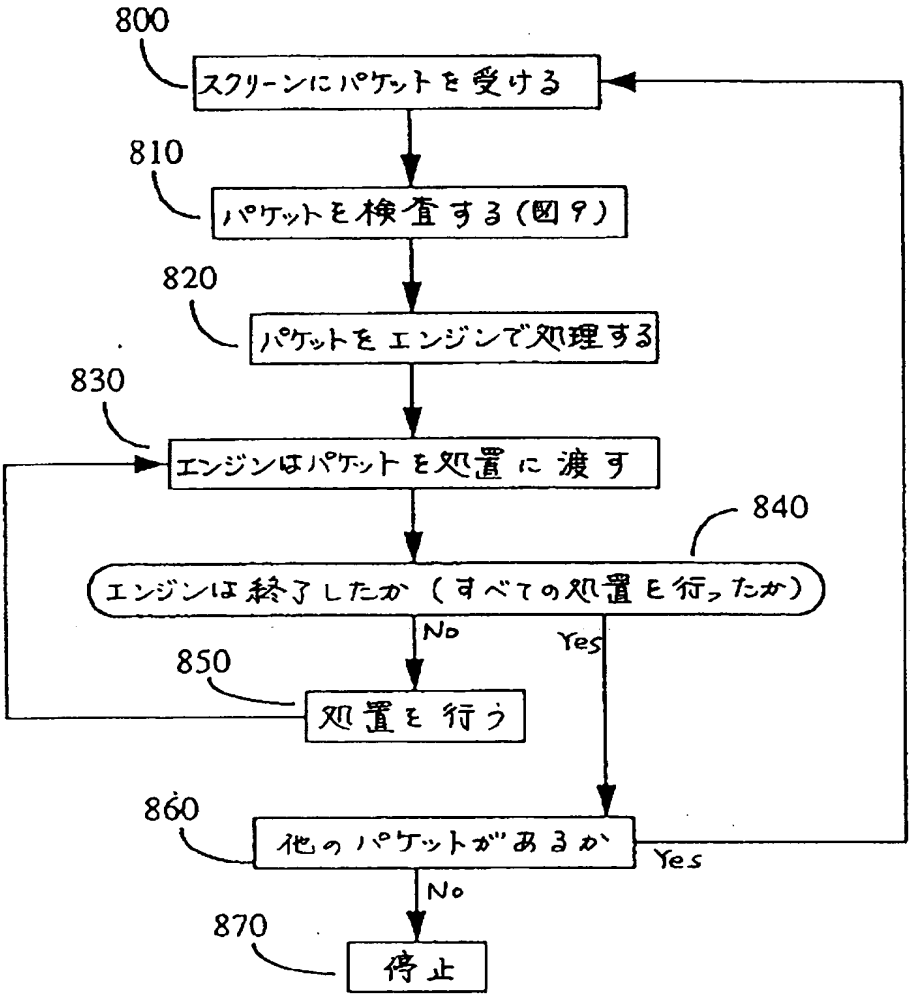

340
520
510
他の記憶装置／メモリ
I/O
500
ディスク記憶装置
メモリ
プロセッサ
400
他のネットワーク・インタフェース
390
A
415
ネットワークインタフェース１
ネットワークインタフェース
410
ネットワークインタフェース２
427
420
(他のプライベートネットワーク)
337
プライベートネットワーク
代行ネットワーク
公衆ネットワーク
335
330
430
350
355

530
540
550
560
プライベートネットワーク
スクリーンシステム
公衆ネットワーク
B

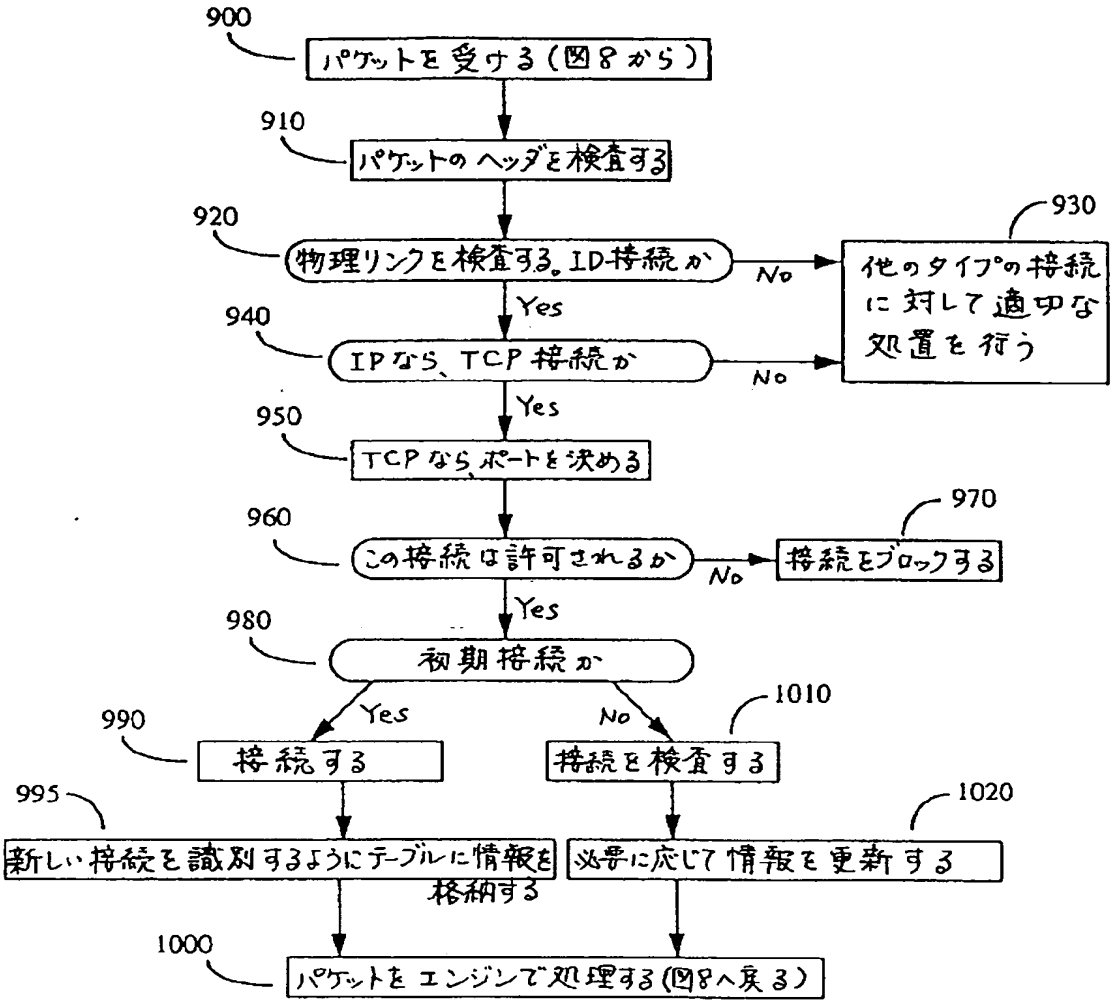
【図９】


パケット状態テーブル
650
処置
ログファイル記憶
640
630
610
675
Fragmentation Bypass
分割機能
660
エンジン
規則
620
キャッシュ分割
670
600
パケット検査
602
604
606
680
学習ブリッジ・テーブル
NI1プロセス
NI2プロセス
NI3プロセス
425
ネットワーク・インタフェース1
410
ネットワーク・インタフェース2
420
ネットワークインタフェース3
340
プライベートネットワーク
330
代行ネットワーク
430
公衆ネットワーク
350

【図１０】


800
スクリーンにパケットを受ける
810
パケットを検査する（図９）
820
パケットをエンジンで処理する
830
エンジンはパケットを処置に渡す
840
エンジンは終了したか（すべての処置を行ったか）
No
Yes
850
処置を行う
860
他のパケットがあるか
Yes
No
870
停止

【図１１】



フロントページの続き

(72)発明者　ウィリアム・ダニエルソン
アメリカ合衆国　94040　カリフォルニア州・マウンテンビュー・カトリーナ　ウェイ・2728
(72)発明者　トーマス・エル・ライアン
アメリカ合衆国　94301　カリフォルニア州・パロ　アルト・エッジウッド　ドライブ・1400
(72)発明者　ジェフリー・マリガン
アメリカ合衆国　94555　カリフォルニア州・フレモント・ウィンブラル　コート・3330
(72)発明者　マーティン・パターソン
フランス国　38000グルノーブル・リュドゥ　ボストン・５
(72)発明者　グレン・シイ・スコット
アメリカ合衆国　93561　カリフォルニア州・テハチャピ・ムーン　ドライブ・19700
(72)発明者　キャロライン・タービフィル
アメリカ合衆国　95030　カリフォルニア州・ロス　ガトス・アーモンド　ヒル　コート・105